TEORIA DEI NUMERI (ADVANCED?)

Titolo nota 04/09/2013

$$\mathbb{Z}[i] = \{ a+bi \mid a, b \in \mathbb{Z} \}$$

$\mathbb{Z}/6\mathbb{Z}$ è un anello, ma non è $\left\{ \begin{array}{l} \text{un dominio integro} \\ \text{d. integrità} \end{array} \right.$

$$(5) = (2+i)(2-i)$$

IRRIDUCIBILI vs PRIMI

Primo p se $p \mid ab \Rightarrow p \mid a$ o $p \mid b$

e p non è invertibile

Dividere? $ab = p \cdot (\text{qualcos'altro})$

Irriducibile $p = a \cdot b \Rightarrow a$ è invertibile o b è invertibile

p non invertibile

Negli interi di Gauss, $1+i = i \cdot (1-i)$

$3+4i$ non è invertibile in $\mathbb{Z}[i]$, perché

$(3+4i)^{-1} = \dfrac{3-4i}{25}$ non è un intero di Gauss

Es (invertibili in $\mathbb{Z}[i]$)

$(a+bi)$ è invertibile? Il suo inverso (in $\mathbb{C}$)

è $\dfrac{a-bi}{a^2+b^2}$, che sta in $\mathbb{Z}[i]$ $\Longleftrightarrow$

$$\frac{a}{a^2+b^2} \in \mathbb{Z}, \qquad -\frac{b}{a^2+b^2} \in \mathbb{Z}$$

$\Longleftrightarrow$ $a=0,\ b=\pm 1$ oppure $a=\pm 1,\ b=0$

SEMPRE: primo $\Longrightarrow$ irriducibile

$$p = a \cdot b \implies p \mid a \implies a = Kp$$

$$p = b \cdot K \cdot p$$

$\xRightarrow{\text{dominio}}$ $1 = b \cdot K$

ATTENZIONE! Il contrario è falso: lavoriamo in $\mathbb{Z}[\sqrt{-5}]$ ed osserviamo che

$$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

- 2 è irriducibile

Se potessi scrivere $2 = (a+b\underset{\parallel}{\overset{a+bi\sqrt{5}}{}}\sqrt{-5})(c+d\sqrt{-5})$,

otterrei $4 = (a^2+5b^2)(c^2+5d^2)$

$\Rightarrow$ $b=0$ e $d=0$

$\Rightarrow \quad 2 = a \cdot c$ dove $a, c \in \mathbb{Z}$

- 2 non e' primo: $2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$

ma $2 \nmid 1+\sqrt{-5}$, $2 \nmid 1-\sqrt{-5}$: l'equazione

$$1+\sqrt{-5} = 2\left(a + b\sqrt{-5}\right)$$

non ha soluzioni

$x^2 + 1 = y^3$

$(x+i)(x-i) = y^3$

Domanda zero: $x+i$ e $x-i$ sono primi tra loro?

Oss: x è pari, altrimenti assurdo mod 4

y è dispari

Prendiamo un divisore comune di $x+i$, $x-i$.
Lo chiamo δ.

$$\delta \mid (x+i)-(x-i) = 2i$$

$\delta \mid 2i \iff \delta \mid 2$

$\Updownarrow \qquad\qquad \Updownarrow$

$2i = \alpha \cdot \delta \qquad 2 = \beta \cdot \delta$

$\Leftrightarrow$

$2 = (-i\alpha) \cdot \delta$

LE UNITÀ NON CONTANO NEI RAGIONAMENTI DI DIVISIBILITÀ

D'altro canto $\delta \mid (x+i)(x-i) = y^3$

$\delta \mid 2$

$$\begin{cases} \text{Norma}(\delta) \mid \text{Norma}(y^3) = y^6 \\ \text{Norma}(\delta) \mid N(2) = 4 \end{cases}$$

Siccome y è dispari, $N(\delta) = \pm 1$, e anzi fa $+1$, perché sicuramente $N(\delta) \geq 0$

NORMA

- $N(a+bi) = a^2+b^2$

- $\alpha \mid \beta \Rightarrow N(\alpha) \mid N(\beta)$

Perché? Se $\beta = \alpha\gamma$, prendendo i moduli (come numeri complessi) trovo $|\beta| = |\alpha| \cdot |\gamma|$ e facendo il quadrato $N(\beta) = N(\alpha) \cdot N(\gamma)$

- $N(3+4i) = 25$

FATTO Se $N(\alpha) = 1$, α è invertibile

Infatti:

$$1 = N(\alpha) = \alpha \cdot \overline{\alpha}$$

e $\overline{\alpha}$ è ancora un intero di Gauss

Quindi $(x+i, x-i) = 1$, e quindi

ognuno è un cubo

Ma se $(x+i)$ è un cubo, $\exists\, a+bi$:

$$x+i = (a+bi)^3$$

Confrontando le parti immaginarie,

$$1 = 3a^2b - b^3$$
$$= b(3a^2-b^2),$$

dunque $b = \begin{cases} +1 & \Longrightarrow \text{ non riesco a trovare } a \\ -1 & \Longrightarrow a = 0 \end{cases}$

Quindi $x+i = (-i)^3$, cioè $x=0$

$x+i$ è un cubo <u>a meno di unità</u>, ma in $\mathbb{Z}[i]$ tutte le unità sono cubi: $(-i)^3 = i$

COS'È LA FATTORIZZAZIONE UNICA?

Si dice che un anello ha fatt. unica se ogni suo elemento si scrive in modo unico come prodotto di irriducibili

A MENO DI UNITÀ

Es $2 = (1+i)(1-i) = -i(1+i)^2$

Fatto α è un'unità in $\mathbb{Z}[\sqrt{-d}]$ se e solo se $N(\alpha)=1$.

Se $\alpha \cdot \alpha^{-1} = 1$

$$N(\alpha) \cdot N(\alpha^{-1}) = 1$$

Siccome $N(\alpha)$, $N(\alpha^{-1})$ sono interi >0,

$N(\alpha)=1$

Viceversa, $1 = N(\alpha) = \alpha \cdot \overline{\alpha}$

Perché in $\mathbb{Z}$ irriducibile $\Rightarrow$ primo?

Sia p irriducibile, $p \mid ab$, vogliamo dimostrare $p \mid a$ oppure $p \mid b$.

Per assurdo questo non succede.

$(a, p) = 1$ $\qquad\qquad$ $(b, p) = 1$ Bézout

$ha + kp = 1$ $\qquad\qquad$ $h'b + k'p = 1$

Moltiplicando membro a membro,

$$p(\ldots) + \underbrace{hh'ab}_{\text{divisibile per } p} = 1,$$

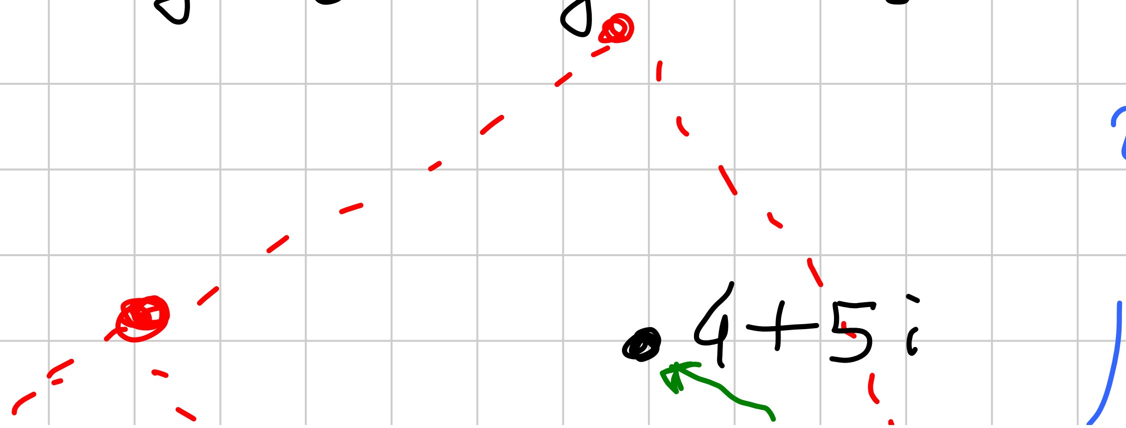
e quindi $p \mid 1$, assurdo.

Come si dimostra Bézout? Con Euclide.

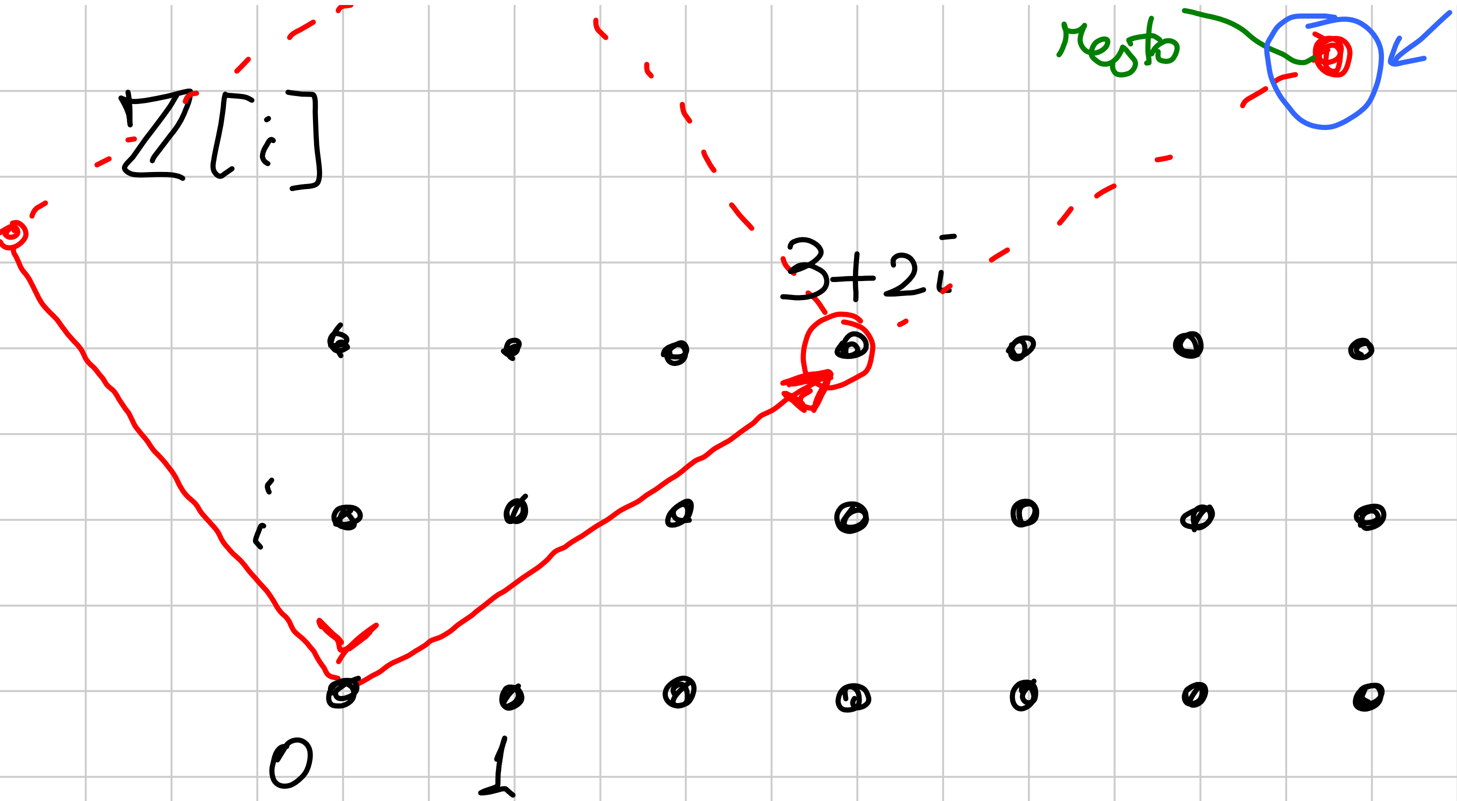
La divisione con resto vuol dire che ho una certa quantità ("la grandezza" delle cose in gioco) e per ogni a e b so scrivere $a = kb + r$ con il resto che è o zero o più piccolo di b.

Sostengo che $\mathbb{Z}[i]$ ha la divisione euclidea con "funzione grandezza" la norma

vertice più vicino a $4+5i$



$\mathbb{Z}[i]$



Dividiamo $4+5i$ per $3+2i$

Lato dei quadrati rossi $= N(3+2i)^{1/2}$

Se prendo il vertice del reticolo rosso più vicino alla cosa che sto dividendo, la distanza fra questi due punti è $\leq \frac{N(3+2i)^{1/2}}{\sqrt{2}}$

E se non c'è la fattorizzazione unica?

$$y^2 = x^3 - 26$$

$\boxed{x = 3 \text{ e } y = 1}$

$$(y + \sqrt{-26})(y - \sqrt{-26}) = x^3$$

Saranno coprimi? Se $\delta \mid (y + \sqrt{-26},\ y - \sqrt{-26})$: allora

$$\delta \mid 2\sqrt{-26} \implies N(\delta) \mid 8 \cdot 13$$

D'altro canto, $\delta \mid x^3 \implies N(\delta) \mid x^6$

Congruenze mod 13^k e mod 4 dicono che

$$(x, 26) = 1, \quad \text{da cui } N(\delta) = 1$$

$N(a + b\sqrt{-26}) = a^2 + 26b^2$, quindi $N = 1$

$\iff a = \pm 1, \ b = 0$

Quindi $y + \sqrt{-26} = (a + b\sqrt{-26})^3$ e quindi

$$1 = 3a^2 b - 26 b^3$$

Allora $b = \pm 1$ e

$b = 1 \quad a = \pm 3$

$b = -1 \quad$ assurdo

$$y = a^3 + 3a(-26b^2) = 27 - 78 \cdot 3$$
$$= -207$$

$x = 35$

Usando la fattorizzazione unica, che però è falsa, abbiamo

* trovato la soluzione $(35, \pm 207)$ <u>OK</u>

* dimostrato che è l'unica <u>MALE</u>

La dimostrazione è, naturalmente, completamente falsa.

Esempio $x^2+2=3^n$, n dispari

Fatto $\mathbb{Z}[\sqrt{-2}]$ ha fattorizz. unica

$$(x+\sqrt{-2})(x-\sqrt{-2}) = (1+\sqrt{-2})^m(1-\sqrt{-2})^n$$

$$\delta \mid x+\sqrt{-2}, \quad \delta \mid x-\sqrt{-2} \quad \Rightarrow \quad \delta \mid 2\sqrt{-2}$$

$$N(\delta) \mid 8$$

$$N(\delta) \mid 3^{2m} \quad \Rightarrow N(\delta)=1, \ \delta \text{ è una unità}$$

Tutte le unità sono potenze n-esime.

$$\overset{\{\pm 1\}}{\shortparallel}$$

$1+\sqrt{-2}$ è primo? Siccome c'è fatt. unica, è suff. vedere che è irriducibile.

Supponiamo $1+\sqrt{-2} = \alpha \cdot \beta$. Allora

$$3 = N(1+\sqrt{-2}) = N(\alpha)\cdot N(\beta),$$

e quindi (WLOG) $N(\beta)=1$.

Le cose di norma 1 sono unità, quindi la fattorizzazione era falsa

In generale $N(\alpha)=p$ primo $\Rightarrow$ α irrid.

Quindi $x \pm \sqrt{-2} = (1 \pm \sqrt{-2})^n$ (non necess. con lo stesso segno)

Attenzione ai segni! ($x \longleftrightarrow -x$ se serve)

$$\pm 2\sqrt{-2} = (1+\sqrt{-2})^n - (1-\sqrt{-2})^n$$

Lavoriamo modulo $(1-\sqrt{-2})$.

Troviamo $\pm 2\sqrt{-2} \equiv (1+\sqrt{-2})^n \pmod{1-\sqrt{-2}}$

cioe' $\pm 2 \equiv 2^n \pmod{1-\sqrt{-2}}$

$\Rightarrow \quad 4 \equiv 2^{2n} \pmod{1-\sqrt{-2}}$

$$(1-\sqrt{-2}) \mid (4^n - 4)$$

Quindi $4^n - 4 = (1-\sqrt{-2})\,\alpha$, da cui

$$4^n - 4 = (1+\sqrt{-2})\,\overline{\alpha},$$

e cioe' $4^n \equiv 4 \pmod{1+\sqrt{-2}}$

$$\text{COPRIMI}\begin{cases} (1+\sqrt{-2}) \mid 4^n-4 \\ (1-\sqrt{-2}) \mid 4^n-4 \end{cases} \Longrightarrow (1+\sqrt{-2})(1-\sqrt{-2}) \mid 4^n-4$$

$$\Longrightarrow 3 \mid 4^n-4$$

Ci è andata male. Proviamo mod $(1-\sqrt{-2})^2$.

$$\pm 2\sqrt{-2} = (1+\sqrt{-2})^n - (1-\sqrt{-2})^n$$

$$\pm 2\sqrt{-2} \equiv (1+\sqrt{-2})^n \quad \left(\bmod\ (1-\sqrt{-2})^2\right)$$

$$(1-\sqrt{-2})^2 = -2\sqrt{-2}-1 \qquad (\text{Suppongo } n \geq 2)$$

$$\mp 1 \equiv (1+\sqrt{-2})^n \quad \left(\operatorname{mod} (1-\sqrt{-2})^2\right)$$

$$1 \equiv (2\sqrt{-2}-1)^n \quad (\quad '' \quad)$$

$$1 \equiv (-2)^n \quad \operatorname{mod} \ (\quad)^2$$

Grazie alla divisibilità per il compl. coniug.,

$$1 \equiv (-2)^n \pmod 9$$

$\mathrm{ord}_9(-2) = 3$, quindi $3 \mid n$

Ma se $3 \mid n$ tanto vale risolvere

$$x^2 + 2 = y^3$$

Questa si fa come prima... $x=5$, $y=3$

I MALEFICI $\mathbb{Z}\left[\frac{\sqrt{n}+1}{2}\right]$

$\mathbb{Z}[\sqrt{n}]$

Gli $n \equiv 1 \pmod 4$ sono problematici.

$n = 5$ $\qquad (1+\sqrt{5})(1-\sqrt{5}) = -4$

$= -2 \cdot 2$

$\varphi = \frac{1+\sqrt{5}}{2}$ $\qquad \varphi^2 - \varphi - 1 = 0$

Norma $(a+b\sqrt{n}) = (a+b\sqrt{n})(a-b\sqrt{n})$

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

$$N\left(\frac{1+\sqrt{n}}{2}\right) = \frac{1-n}{4} \in \mathbb{Z} \quad \text{se} \quad n \equiv 1\ (4)$$

$$\frac{1+\sqrt{n}}{2} + \frac{1-\sqrt{n}}{2} = 1$$

Se $n \equiv 1 \ (4)$, $\mathbb{Z}[\sqrt{n}]$ non è MAI a fattorizzazione unica.

Quello che ha speranze è $\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right] =$

$$= \left\{ a + b\,\frac{1+\sqrt{n}}{2} \;\middle|\; a, b \in \mathbb{Z} \right\}$$

$\mathbb{Z}[\sqrt{-3}]$ non è a fatt. unica

$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\zeta_6] = \mathbb{Z}[\zeta_3]$$

$= \mathbb{Z}[\omega]$ è a fatt. unica

"interi di Eisenstein"

Cose a fatt. unica

$n < 0 \qquad n = -1, -2, -3, -7, -11,$

$-19, -43, -67, -163$

$\mathbb{Z}[i], \ \mathbb{Z}[\zeta_3], \ \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right], \ldots$

$n > 0$ $n = 2, 3, 5, 6, \ldots$?

Eq. di RAMANUJAN $x^2+7=2^n$

$\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ ha fatt. unica

$n \leq 2$ o n pari ve la fate.

$$\frac{x^2+7}{4} = 2^y$$

$$= \left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right)$$